Глава 2.

3 билет. Алгоритм Евклида. Следствия из алгоритма Евклида

Алгоритм Евклида: общая запись.

Пусть есть два числа $a, b \in \mathbb{N}, a > b$. Будем делить с остатком и при этом использовать остаток от деления первого числа для второго. Все числа здесь принадлежат $\mathbb{N}$.
r_i - это остаток, а q_j - это целый множитель.

$$a = b \cdot q_1 + r_1$$
$$b = r_1 \cdot q_2 + r_2$$
$$r_1 = r_2 \cdot q_3 + r_3$$
$$\vdots$$
$$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$$
$$r_{n-2} = r_{n-1} \cdot q_n + 0$$

При этом целые части q_i нам вообще не важны: мы используем только остатки. Основная суть этого алгоритма это использование предыдущего остатка r_{i-1} от деления в следующем шаге как множитель, вместе с новым каким-то числом для получения нового, важного нам, остатка, пока не получим 0.

Теорема 2.
Всегда последний ненулевой остаток (r_{n-1}) будет НОД двух чисел a, b.

Для доказательства заметим, что последовательность множителей $\{b, r_1, r_2, r_3, \cdots, r_{n-1}\}$ всегда убывает (строго). А значит мы не можем делать эти шаги бесконечно, а также последним шагом будет ноль.

Пусть d будет общим делителем a, b, тогда $a \vdots d$ и $b \vdots d$. Так как $a \vdots d$, то и $(b \cdot q_1 + r_1) \vdots d$ по первому равенству. А значит левую часть можно представить как $d \cdot$ (какое-то целое число). Тогда можно заметить, что остаток r_1 тоже должен делится на d, чтобы можно было вынести d за скобки. Так как мы знаем, что b, r_1 делятся на d, то и r_2 будет делится на d, если мы проделаем все то же самое. Мы можем так продолжать до r_{n-1}. В общем, $OD(a, b) = OD(b, r_1) = \cdots = OD(r_{n-2}, r_{n-1}) = OD(r_{n-1}, 0) = r_{n-1}$, так как для любого $a, OD(a, 0) = a$ (можно вспомнить свойство два НОД'а). Так как у них совпадают общие делители не сложно понять, что больший из них тоже будет совпадать. Ура, получилось.

Теорема 3
Пусть $a, b, m \in \mathbb{N}$. Тогда $(a \cdot m, b \cdot m) = m \cdot (a, b)$.

При этом m может принадлежать $\mathbb{Q}$, если числитель и знаменатель $\in OD(a, b)$.

Пример: $(14, 4) = 2 \cdot (7, 2) = 2 \cdot 1 = 2$. или $(7, 2) = (\frac{14}{2}, \frac{4}{2}) = \frac{(14,4)}{2} = \frac{2}{2} = 1$

Доказательство

- Если $m \in \mathbb{N}$:

  Рассмотрим алгоритм Евклида: $a \cdot m = m \cdot (b \cdot q_1 + r_1) = b \cdot m \cdot q_1 + r_1 \cdot m$. Так как остаток r_1 умножается на m, этот множитель сохранится вплоть до r_{n-1}, а значит $r_{n-1} \cdot m = (a, b) \cdot m$.

- Если $m \in \mathbb{Q}$ и $m = \frac{1}{n}, n \in \mathbb{N}$.

  Так как $n \in OD(a, b)$ то число будет все равно в $\mathbb{Z}$ и мы повторяем шаги из первого случая.

4 билет. Линейное представление НОД

Теорема 4

Пусть $a, b \in \mathbb{Z}$. Тогда существуют такие $x, y \in \mathbb{Z}$, что $(a, b) = ax + by$. Это называется линейным представлением НОДа.

Доказательство.

- Сначала приведем числа к виду удобному для алгоритма Евклида. Так как делители у чисел a и $-a$ одни и те же, $(a, b) = (a, -b)$. Поэтому, можно считать, что $a, b \in \mathbb{N}$.
- НУО $a \geqslant b$. Воспользуемся алгоритмом Евклида и соответствующими обозначениями, дополним их: пусть $r_0 = b$ и $r_{-1} = a$.
- Докажем по задне приводной индукции, для Л.П. будем брать рядом стоящие остатки. База $k = n$: $(a, b) = 1r_{n-1} + 0$.
  Переход $k \to k - 1$. Из алгоритма Евклида мы знаем, что
  $r_{k-2} = r_{k-1} \cdot q_k + r_k \Rightarrow r_k = r_{k-2} - r_{k-1} \cdot q_k$.
- Подставим:
  $(a, b) = x_k \cdot r_k + y_k r_{k-1} = x_k \cdot (r_{k-2} - r_{k-1} \cdot q_k) + y_k \cdot r_{k-1} = (-x_k \cdot q_k + y_k) r_{k-1} + x_k \cdot r_{k-2}$.
- То есть мы перешли к предыдущему номеру остатка, карабкаясь вверх. Значит существует Л.П. для каждой пары рядом стоящих остатков, в том числе a и b. (мы их обозначили как остатки номеров -1 и 0).

5 билет. НОД нескольких чисел через НОД двух чисел. Линейное представление НОД нескольких чисел.

Чтобы взять НОД нескольких чисел $a_1, a_2, \dots, a_n \in \mathbb{N}$ Нужно брать НОД чисел попарно. $(a_1, a_2, a_3) = ((a_1, a_2), a_3)$

Тогда мы ищем НОД только двух чисел, а по алгоритму Евклида такое действие определено.

Примеры:
1) $(2, 4, 6, 8) = ((2, 4), 6, 8) = (2, 6, 8) = ((2, 6), 8) = (2, 8) = 2$.
2) $(1, 3, 7) = ((1, 3), 7) = (1, 7) = 1$

Пусть есть $a_1, a_2, \dots a_n$, где $n > 2$. Тогда разобъем их попарно и положим в m_i: $m_2 = (a_1, a_2), m_3 = (a_2, a_3), \cdots, m_n = (a_{n-1}, a_n)$..

Теорема 5
После разбиения попарно выше, $m_n = (a_1, a_2, \dots a_n)$. и $OD(m_n) = OD(a_1, a_2, \dots a_n)$.

Доказательство

- Докажем индукцией по количеству элементов k.

  База $k = 2$ доказана с помощью Алгоритма Евклида.

  Переход $k \to k + 1$:

  $OD(a_1, a_2, \dots a_k, a_{k+1}) = OD(OD(a_1, a_2, \dots a_k), a_{k+1}) = OD(OD(m_k), a_{k+1}) = OD(m_k, a_{k+1}) = OD(m_{k+1})$
- Переход сработал, так что верно, что $OD(m_n) = OD(a_1, a_2, \dots, a_n) \Rightarrow m_n = (a_1, a_2, \dots, a_n)$.

Следствие

Для $a_1, a_2, \dots, a_n \in \mathbb{Z}$ существует Л.П. НОД, то есть, такие $x_1, x_2 \dots, x_n \in \mathbb{Z}$, что $(a_1, a_2, \dots, a_n) = x_1 \cdot a_1 + x_2 \cdot a_2 + \dots + x_n \cdot a_n$.

Доказательство

- Докажем индукцией по количеству элементов k.

  База $k = 2$ Доказана в Теореме 4. (Л.П. двух чисел).

  Переход $k \to k+1$:

  Воспользуемся Теоремой 5.

  $(a_1, a_2, \dots, a_k, a_{k+1}) = (m_k, a_{k+1})$.

  Представим первую скобку в виде Л.П. для y и x_{k+1}:

  $(m_k, a_{k+1}) = y \cdot m_k + x_{k+1} \cdot a_{k+1}$

  Раскроем m_k по ее определению из Теоремы 5 и применим индукционное предположение, где множителями будут $x_1, x_2, \dots, x_k$.

  $(a_1, a_2, \dots, a_{k+1}) = y \cdot m_k + x_{k+1} \cdot a_{k+1} = y \cdot (x_1 \cdot a_1 + x_2 \cdot a_2 + \dots + x_k \cdot a_k) + x_{k+1} \cdot a_{k+1}$

  Раскроем скобки

  $(a_1, a_2, \dots, a_{k+1}) = y \cdot m_k + x_{k+1} \cdot a_{k+1} = (y \cdot x_1) \cdot a_1 + (y \cdot x_2) \cdot a_2 + \dots + (y \cdot x_k) \cdot a_k + x_{k+1} \cdot a_{k+1}$

- Сейчас в скобках нужные нам коэффициенты для Л.П. и, так как сработал индукционный переход, существует Л.П. для НОДа сразу нескольких чисел.